9405 SW Gemini Drive, Beaverton, OR 97008 USA
T. +1 503.469.4800 F. +1 503.469.4777 www.digimarc.com

FACSIMILE TRANSMITTAL

DATE: November 2, 2005

TO: Commissioner of Patents

FAX 571-273-8300

FROM: Steven W. Stewart

PAGES: 22 (including cover)

RE: U.S. Patent Application No. 09/858,336

FILED: May 15, 2000

FOR: IMAGE MANAGEMENT SYSTEM AND METHODS USING DIGITAL WATERMARKS

ART UNIT: 2672

DOCKET NO.: P0366

✓ Urgent ☐ For Review ☐ Please Reply

FACSIMILE COVER LETTER

Attached is an Appeal Brief and Transmittal Letter with deposit account authorization for the above referenced application.

CERTIFICATE OF FAXING

I hereby certify that these papers are being facsimile transmitted to the US Patent Office, 571-273-8300 on November 2, 2005.

Steven W. Stewart, Reg. No. 45,133
Attorney for Applicant

If you do not receive all pages or if you have problems receiving transmittal, please call us at 503-469-4800.

SWS:lmp 11/2/05 P0366

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Philip R. Patterson

Application No.: **09/858,336**

Filed: May 15, 2000

For: IMAGE MANAGEMENT SYSTEM AND METHODS USING DIGITAL WATERMARKS

Examiner: Jin Cheng Wang

Date: November 2, 2005

Response Under 37 CFR § 1.116
Expedited Procedure

Art Unit: 2672

Confirmation No.: 1102

CERTIFICATE OF TRANSMISSION

I hereby certify that this paper and the documents referred to as being attached or enclosed herewith are being facsimile transmitted to the United States Patent and Trademark Office at 571-273-8300 on November 2, 2005.

Steven W. Stewart
Attorney for Applicants

TRANSMITTAL LETTER

MAIL STOP APPEAL BRIEF – PATENTS
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

Enclosed for filing in the above-captioned matter are the following:

☒ Appeal Brief (fee **$500.00**)

☒ Applicant petitions for a four month extension of time from July 4, 2005 to November 4, 2005 (fee of **$1,590.00**). If any additional extension of time is required, please consider this a petition therefor.

☒ Please charge **$2,090.00** (fee for Appeal Brief and extension of time) and any additional fees which may be required in connection with filing this document and any extension of time fee, or credit any overpayment, to Deposit Account No. 50-1071.

Respectfully submitted,

Date: November 2, 2005

DIGIMARC CORPORATION

CUSTOMER NUMBER 23735

Phone: 503-469-4800
FAX 503-469-4777

By_____
Steven W. Stewart
Registration No. 45,133

11/03/2005 AKELECH1 00000016 501071 09858336

01 FC:1254 1590.00 DA

SWS:lmp 11/2/05 P0366

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Philip R. Patterson

Application No.: **09/858,336**

Filed: May 15, 2000

For: IMAGE MANAGEMENT SYSTEM AND METHODS USING DIGITAL WATERMARKS

Examiner: Jin Cheng Wang

Date: November 2, 2005

Response Under 37 CFR § 1.116

Expedited Procedure

Art Unit: 2672

Confirmation No.: 1102

CERTIFICATE OF TRANSMISSION

I hereby certify that this paper and the documents referred to as being attached or enclosed herewith are being facsimile transmitted to the United States Patent and Trademark Office at 571-273-8300 on November 2, 2005.

Steven W. Stewart
Attorney for Applicants

APPEAL BRIEF

Mail Stop Appeal Brief – Patents
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Appellants respectfully request the Board of Patent Appeals and Interferences (hereafter the "Board") to reverse the outstanding final rejection of the pending claims.

This Appeal Brief is in furtherance of a Notice of Appeal filed May 4, 2005. Please charge the fee required under 37 CFR 1.17(f) or any needed fee to deposit account 50-1071 (please see the accompanying transmittal letter).

11/03/2005 AKELECH1 00000016 501071 09858336
02 FC:1402 500.00 DA

REAL PARTY IN INTEREST

The real party in interest is Digimarc Corporation, by an assignment from the inventors recorded at Reel 012185, Frames 0036-0038, on September 20, 2001.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

STATUS OF CLAIMS

Claims 9-14, 25-27 and 30-35 are pending in the present application. Each of these claims stand finally rejected. Please see the Office Action Summary in the final Office Action mailed January 11, 2005. (Claims 1-8, 15-24, 28 and 29 have been previously canceled.)

STATUS OF AMENDMENTS

All earlier-filed amendments have been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

The present invention relates generally to steganography, which is the art of hiding information (e.g., plural binary bits) in some other object without leaving human-apparent evidence of the alteration. Please see page 2, paragraph 9 of the subject specification.

One form of steganography is digital watermarking. Digital watermarking may be used to modify media content to embed a message or machine-readable code into the content. The content may be modified such that the embedded code is imperceptible or nearly imperceptible to the user, yet may be detected through an automated detection process. Please see the specification at paragraph 10, spanning pages 2 and 3.

One problem faced by image management systems is how to efficiently manage an image's ancestry and related information. Normal image processing (e.g., scaling, cropping, rotating, clipping, resizing, cut-and-pasting image blocks, and/or marking, etc.) of an "original" image results in a "derivative" image. In conventional systems, derivative images frequently

retain minimal, if any, related metadata. The metadata, such as that stored in header or footer files, is easily separable from derivative images. Separation results in a significant loss of information, particularly for a derivative image. One conventional solution manually records an image identifier as an image moves through an exploitation (or derivative) process. This manual recording process is labor intensive and cumbersome at best. Please see, e.g., page 8, paragraph 32 of the subject specification.

The present invention addresses this and other problems using steganographic and digital watermarking techniques.

One aspect of the invention, as recited in claim 9, is a method for managing images. The images include a first image comprising a first identifier steganographically embedded therein (see, e.g., page 8, lines 1-2 of paragraph 33; see also Fig. 2, image 001 including watermark identifier ID-1). The method includes retrieving a copy of the first image from an image database (see, e.g., page 8, lines 4-5 of paragraph 33; see also Fig. 2, image 001 and database 14); altering the copy of the first image to provide a second image (see, e.g., page 9, paragraph 35 and lines 1-3 of paragraph 36; see also Fig. 2 – image 001 and derivative 001); steganographically embedding a second identifier in the second image (see, e.g., page 9, lines 1-4 and 8-13 of paragraph 36); and providing the steganographically embedded second image to the image database for storage (see, e.g., Fig. 2, database 14 and image 001 (ID-1) and derivative 001; see also page 9, lines 3-5 of paragraph 35, and page 10, lines 1-5 of paragraph 39), wherein the image database associates the second identifier with the first identifier so as to associate the first image and the second image (see, e.g., page 9, lines 3-5 of paragraph 35; see also Fig. 2, database 14 and image family, see also page 10, lines 4-8 of paragraph 39).

Another aspect of the invention, as recited in claim 35 is an apparatus. The apparatus (see, e.g., Fig. 2, database 14) includes electronic processing circuitry and memory (see, e.g., page 17, paragraph 59). The memory includes records stored therein, the records comprising a plurality of images, the plurality of images including a first image (see, e.g., Fig. 2, image 001) and a second image (see, e.g., Fig. 2, derivative 001). The first image includes a first identifier steganographically embedded therein (see, e.g., Fig. 2, ID-1; see also page 8, lines 1-2 of

paragraph 33). And the second image includes a second identifier steganographically embedded therein (see, e.g., Fig. 2, ID-5; see also page 9, lines 1-3 of paragraph 35). The second image is derived from the first image (see, e.g., page 9, last 2 lines of paragraph 34). The second identifier is associated with the first identifier so that the first image and the second image are associated with one another (see, e.g., Fig. 2, database 14 and image family; see also page 9, lines 3-5 of paragraph 35 and page 10, lines 4-8 of paragraph 39).

Yet another aspect of the invention, as recited in claim 25, is a system. The system includes a first user terminal (see, e.g., Fig. 4, terminal 40; see also page 14, paragraph 49), a second user terminal (see, e.g., Fig. 4, terminal 44; see also page 14, paragraph 49) and a database (see, e.g., Fig. 4, database 46; see also page 14, paragraph 49). The first user terminal and the second user terminal are in communication (see, e.g., Fig. 4; see also line 3 of paragraph 49, page 14), and the first user terminal and the second user terminal are each in communication with the database (see, e.g., Fig. 4). The system also includes a gatekeeper to regulate the flow of at least a first image between the first user terminal and the second user terminal (see, e.g., "sentry" 42 shown in Fig. 4 and discussed, e.g., in paragraphs 49-54; see also the flowcharts shown in Fig. 6). The first image comprises at least a first digital watermark including a first identifier (see, e.g., lines 11-17 of paragraph 49 on page 14; see also lines 3-5 of paragraph 50, page 15; and see S20 in Fig. 6). The gatekeeper determines a security level associated with the first image (see, e.g., lines 3-8 of paragraph 50, page 15; see also Fig. 6, S20), compares the first image security level with a user security level (see, e.g., lines 8-10 of paragraph 50 on page 15; see also S22, Fig. 6), and allows access by the second user terminal to the first image based on a result of the comparison (see, e.g., lines 10-12 of paragraph 50 on page 15; see also S24 and S26 in Fig. 6). The gatekeeper includes or communicates with a digital watermark decoder to decode the digital watermark to determine the first identifier (see, e.g., lines 3-5 of paragraph 50, page 15; see also S20, Fig. 6), and to interrogate the database with the first identifier to retrieve the security level (see, e.g., lines 5-7 of paragraph 50, page 15).

Still another aspect of the invention, as recited in claim 26, is a system. The system includes a first user terminal (see, e.g., Fig. 4, terminal 40; see also page 14, paragraph 49), a

second user terminal (see, e.g., Fig. 4, terminal 44; see also page 14, paragraph 49) and a database (see, e.g., Fig. 4, database 46; see also page 14, paragraph 49). The first user terminal and the second user terminal are in communication (see, e.g., Fig. 4; see also line 3 of paragraph 49, page 14), and the first user terminal and the second user terminal are each in communication with the database (see, e.g., Fig. 4). The system also includes a gatekeeper to regulate the flow of at least a first image between the first user terminal and the second user terminal (see, e.g., "sentry" 42 shown in Fig. 4 and discussed, e.g., in paragraphs 49-54; see also the flowcharts shown in Fig. 6). The first image includes at least a first digital watermark including a first identifier (see, e.g., lines 11-17 of paragraph 49 on page 14; see also lines 3-5 of paragraph 50, page 15; and see S20 in Fig. 6). The gatekeeper determines a security level associated with the first image (see, e.g., lines 3-8 of paragraph 50, page 15; see also Fig. 6, S20), compares the first image security level with a user security level (see, e.g., lines 8-10 of paragraph 50 on page 15; see also S22, Fig. 6), and allows access by the second user terminal to the first image based on a result of the comparison (see, e.g., lines 10-12 of paragraph 50 on page 15; see also S24 and S26 in Fig. 6). The first image digital watermark includes security level data (see, e.g., lines 4-5 and 7-8 of paragraph 50, page 15), and wherein said gatekeeper comprises or communicates with a digital watermark decoder to decode the digital watermark to determine the security level data (see, e.g., lines 3-5 and 7-8 of paragraph 50, page 15; see also S20, Fig. 6).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 9-14 and 35 stand finally rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,141,753 (hereafter "the Zhao patent").

2. Claims 25-27 and 30-34 stand finally rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,233,684 (hereafter "the Stefik patent").

ARGUMENT

Appellants respectfully request that the final rejection of the pending claims be reversed since the cited references fail to teach or suggest all of the elements of the pending claims.

Rejections under U.S.C. 102(e) over the Zhao Patent

Claims 9 -13

Independent claim 9 reads as follows:

9. A method for managing images, the images including a first image comprising a first identifier steganographically embedded therein, said method comprising:

retrieving a copy of the first image from an image database;

altering the copy of the first image to provide a second image;

steganographically embedding a second identifier in the second image; and

providing the steganographically embedded second image to the image database for storage, wherein the image database associates the second identifier with the first identifier so as to associate the first image and the second image.

The Examiner argues that it "is clear that there is an association between the second image and the first image because the second image is changed from the first image and ***they share a common fingerprint watermark*** (column 7-8 and 11)." Please see the final Office Action, page 11, lines 7-9 (emphasis added); please also see the final Office Action, page 3, lines 16-18.

But this argument misses the crux of claim 9.

The first and second images of claim 9 have at least different identifiers embedded respectively therein. Claim 9 recites a first image comprising a first identifier steganographically embedded therein (e.g., a first watermark identifier). And a second identifier steganographically embedded (e.g., a second watermark identifier) in a second image.

But this is not all.

The image database associates the second identifier with the first identifier so as to associate the first image and the second image. Please see claim 9, reproduced above.

The mere fact that an image may include a common watermark (or even multiple watermarks) does not imply that a database is associating first and second identifiers to help associate related first and second images.

Moreover, the work storage[1] 105 in the Zhao patent does not associate first and second steganographic (e.g., watermark) identifiers to help associate related first and second images. Rather, the work storage 105 seems to store multiple copies to help reduce a probability that a second encryption key will be lost. Please see Col. 7, lines 33-35 of the Zhao patent.

We respectfully request that the final rejection of claim 9 be reversed.

Claim 35

Independent claim 35 reads as follows:

35. An apparatus comprising:

electronic processing circuitry; and

memory,

said memory comprising records stored therein, the records comprising a plurality of images, the plurality of images including a first image and a second image,

wherein the first image includes a first identifier steganographically embedded therein, and

wherein the second image includes a second identifier steganographically embedded therein,

wherein the second image is derived from the first image, and

wherein the second identifier is associated with the first identifier so that the first image and the second image are associated with one another.

---

1 The work storage 105 is relied upon by the Examiner as teaching an image database. Please see the Office Action at page 3, lines 3-4.

The Examiner argues that it "is clear that there is an association between the second image and the first image because the second image is changed from the first image and ***they share a common fingerprint watermark*** (column 7-8 and 11)." (Emphasis added). Please see the Office Action, page 3, lines 16-18.

But this argument fails to consider the claim language.

The first and second images of claim 35 have at least different identifiers embedded respectively therein. Claim 35 recites a first image comprising a first identifier steganographically embedded therein (e.g., a first watermark identifier). And a second identifier steganographically embedded (e.g., a second watermark identifier) in a second image.

But this is not all.

The second identifier is associated with the first identifier so that the first image and the second image are associated with one another.

The mere fact that an image may include a common watermark (or even multiple watermarks) does not imply that a database is associating first and second identifiers to help associate first and second images.

Moreover, the work storage[2] 105 in the Zhao patent does not associate first and second steganographic (e.g., watermark) identifiers to help associate related first and second images. Rather storing multiple copies in the work storage 105 helps reduce a probability that a second encryption key will be lost. Please see Col. 7, lines 33-35 of the Zhao patent.

We respectfully request that the final rejection of claim 35 be reversed.

---

2 The work storage 105 is relied upon by the Examiner as teaching an image database. Please see the Office Action at page 3, lines 3-4.

Rejections under U.S.C. 102(e) over the Stefik Patent

Claims 25, 27, 31 and 33

Independent claim 25 reads as follows:

25. A system comprising:

a first user terminal;

a second user terminal;

a database, wherein the first user terminal and the second user terminal are in communication, and the first user terminal and the second user terminal are each in communication with the database; and

a gatekeeper to regulate the flow of at least a first image between the first user terminal and the second user terminal, wherein the first image comprises at least a first digital watermark including a first identifier, said gatekeeper to determine a security level associated with the first image, compare the first image security level with a user security level, and to allow access by the second user terminal to the first image based on a result of the comparison, wherein said gatekeeper comprises or communicates with a digital watermark decoder to decode the digital watermark to determine the first identifier, and to interrogate the database with the first identifier to retrieve the security level.

Claim 25 recites a digital watermark decoder to decode a digital watermark to determine a first identifier. The first identifier is used to interrogate a database to retrieve a security level. The retrieved security level is used to determine whether to allow access by a second user terminal to a first image through comparison with a user security level.

The Examiner argues that, data extracted from a watermark and used to identify ***who and where*** an unauthorized reproduction of digital work came from, meets this limitation. Please see page 8, lines 1-3, of the final Office Action.

We respectfully disagree. The Examiner's position simply ignores the claimed feature of database interrogation with the first identifier to retrieve a security level. (The Examiner's

position does not even suggest that a security level is determined at all; but, rather, implies simple user identification, e.g., "who and where".)

The Examiner further notes that a watermark is sent through a trust box where a printer server is allowed to print an image for a given security level. Please see page 8, lines 3-7, of the final Office Action (citing cols. 9 and 12-16 of the Stefik patent).

Even if the Stefik patent does disclose this teaching (which we do not concede), there is still no discussion of how a decoded watermark identifier is used to interrogate a database to retrieve a security level, and how this retrieved security level is used to control access to a first image.

Moreover, we do not read the cited passages of the Stefik patent (i.e., cols. 9 and 12-16) in this manner.

Although the Examiner cites six (6) columns for these features[3], we see reference to a trust box starting in col. 14, line 13. According to the Stefik patent, watermark data is obtained from a digital certificate provided by a user and printer. See Col. 15, lines 8-11. In other words, a digital certificate (common in encryption schemes) itself *contains* the watermark information. See the final Office Action at page 12, lines 16-17. A watermark font is then downloaded to a printer for use when printing a book. See Col. 15, lines 11-13.

But these passages do not seem terribly helpful for the features at issue. That is, there is no discussion of decoding a digital watermark to determine a first identifier, which is used to interrogate a database to retrieve a security level. The retrieved security level is used to determine whether to allow access by a second user terminal to a first image through comparison with a user security level.

At best the Col. 15 passage of the Stefik patent discusses providing a watermark font to a printer through a trust box. Please see, e.g., Col. 15, lines 11-13. The printer will use the font when printing a book.

---

3 To be clear, the features at issue include using a decoded watermark identifier to interrogate a database to retrieve a security level, and using this retrieved security level to help control access to a first image.

But, in this regard, please recall that claim 25 envisions handling an image that is already watermarked ("*wherein the first image comprises at least a first digital watermark including a first identifier*").

The cited passages in the Stefik patent seem concerned with delivering a font to watermark a book when printing.

We respectfully request that the final rejection of claim 25 be reversed.

Claims 26, 30, 32 and 34

Independent claim 26 reads as follows:

26. A system comprising:

a first user terminal;

a second user terminal;

a database, wherein the first user terminal and the second user terminal are in communication, and the first user terminal and the second user terminal are each in communication with the database; and

a gatekeeper to regulate the flow of at least a first image between the first user terminal and the second user terminal, wherein the first image comprises at least a first digital watermark including a first identifier, said gatekeeper to determine a security level associated with the first image, compare the first image security level with a user security level, and to allow access by the second user terminal to the first image based on a result of the comparison, wherein said first image digital watermark includes security level data, and wherein said gatekeeper comprises or communicates with a digital watermark decoder to decode the digital watermark to determine the security level data.

The Examiner cites the Stefik patent at Col. 17 as teaching "different levels of encryption and 'scrambling'". Please see the Office Action at page 8, lines 13-15.

This alleged teaching is applied against the claim feature of a first image digital watermark including security level data. (Or said another way, the digital watermark itself

carries security level data.)

We have carefully studied Col. 17 of the Stefik patent – it is only 17 lines long.

We read this Col. 17 passage as discussing encrypting or scrambling a document at different stages in a server.

What is missing, however, is any discussion of how this encryption or scrambling information is carried in a digital watermark.

There may be a misunderstanding of the technology involved in claim 26, some confusion between encryption and digital watermarking.

As discussed at page 2, paragraph 9, of the subject specification, digital watermarking is a form of steganography that encompasses a great variety of techniques by which plural bits of digital data are hidden in some other object without leaving human-apparent evidence of alteration. In paragraph 12 (page 3 of the specification) we teach that a watermark embedding component embeds a watermark pattern by altering data samples of the media content. These changes might be through subtle alteration of pixel values or through alteration of DCT or wavelet coefficients, etc. After watermarking, the content appears generally unchanged, as the watermark is imperceptibly hidden in the content.

With encryption, however, the content becomes illegible and incoherent to a human observer.

The discussion of different levels of encryption or scrambling at Col. 17 of the Stefik patent does not teach or suggest that security level data is carried or included in a digital watermark.

We respectfully request that the final rejection of claim 25 be reversed.

CONCLUSION AND REQUEST FOR REVERSAL

The cited references collectively fail to disclose all of the limitations of the pending claims. (Other deficiencies of the art need not be further belabored at this time.) As such, the claims are patentable over the cited references.

Appellants respectfully request that the Board reverse the final rejection of the pending claims.

Respectfully submitted,

Date: November 2, 2005

DIGIMARC CORPORATION

Customer No. 23735

Telephone: 503-469-4685
FAX: 503-469-4777

By _____
Steven W. Stewart
Registration No. 45,133

CLAIMS APPENDIX

1–8. (canceled).

9. (previously presented): A method for managing images, the images including a first image comprising a first identifier steganographically embedded therein, said method comprising:

retrieving a copy of the first image from an image database;

altering the copy of the first image to provide a second image;

steganographically embedding a second identifier in the second image; and

providing the steganographically embedded second image to the image database for storage, wherein the image database associates the second identifier with the first identifier so as to associate the first image and the second image.

10. (previously presented): The method according to claim 9, further comprising removing the first identifier from the second image.

11. (previously presented): The method according to claim 9, further comprising altering the first identifier in the second image.

12. (previously presented): The method according to claim 9, further comprising storing information related to the first image in the database.

13. (original): The method according to claim 12, wherein the related information comprises at least one of metadata, location, date, permission level, security access levels, analyst comments, notes, files, and past usage information.

14. (original): The method according to claim 13, wherein the database comprises a plurality of databases.

15-24. (canceled).

25. (previously presented): A system comprising:

a first user terminal;

a second user terminal;

a database, wherein the first user terminal and the second user terminal are in communication, and the first user terminal and the second user terminal are each in communication with the database; and

a gatekeeper to regulate the flow of at least a first image between the first user terminal and the second user terminal, wherein the first image comprises at least a first digital watermark including a first identifier, said gatekeeper to determine a security level associated with the first image, compare the first image security level with a user security level, and to allow access by the second user terminal to the first image based on a result of the comparison, wherein said gatekeeper comprises or communicates with a digital watermark decoder to decode the digital

watermark to determine the first identifier, and to interrogate the database with the first identifier to retrieve the security level.

26. (previously presented): A system comprising:

a first user terminal;

a second user terminal;

a database, wherein the first user terminal and the second user terminal are in communication, and the first user terminal and the second user terminal are each in communication with the database; and

a gatekeeper to regulate the flow of at least a first image between the first user terminal and the second user terminal, wherein the first image comprises at least a first digital watermark including a first identifier, said gatekeeper to determine a security level associated with the first image, compare the first image security level with a user security level, and to allow access by the second user terminal to the first image based on a result of the comparison, wherein said first image digital watermark includes security level data, and wherein said gatekeeper comprises or communicates with a digital watermark decoder to decode the digital watermark to determine the security level data.

27. (previously presented): The system according to claim 25, wherein the user security level comprises at least one of a security level for a user and a security level for a user terminal.

28-29. (canceled).

30. (previously presented): The system according to claim 26, wherein the user security level comprises at least one of a security level for a user and a security level for a user terminal.

31. (previously presented): The system according to claim 25, wherein said gatekeeper records in the database a transmission of the first image from the first user terminal to the second user terminal.

32. (previously presented): The system according to claim 26, wherein said gatekeeper records in the database a transmission of the first image from the first user terminal to the second user terminal.

33. (previously presented): The system of claim 25, further comprising a communications server, wherein the first user terminal and the second user terminal are in communication via said communications server.

34. (previously presented): The system of claim 26, further comprising a communications server, wherein the first user terminal and the second user terminal are in communication via said communications server.

35. (previously presented): An apparatus comprising:

electronic processing circuitry; and

memory,

said memory comprising records stored therein, the records comprising a plurality of images, the plurality of images including a first image and a second image,

wherein the first image includes a first identifier steganographically embedded therein, and

wherein the second image includes a second identifier steganographically embedded therein,

wherein the second image is derived from the first image, and

wherein the second identifier is associated with the first identifier so that the first image and the second image are associated with one another.

PATENT

SWS:lmp 11/2/05 P0366

EVIDENCE APPENDIX

(No Evidence)